A Review of the Integration and Runtime Specification version 4.2

3 May, 2001

Eric L. Krum
NTAG Tech Dir
MITRE
ESC/DIJ, GCCS-AF
Krume@mitre.org

Purpose

- To review the draft Windows 2000 related DII COE guidance

Note: The items presented in this briefing were approved by the previous Chief Engineer. With new leadership in the DII COE any thing you see or hear is subject to change.

Outline

- Background
- Chapter 7
- Chapter 9
- Chapter 6
- Directory Services Chapter
- Appendix B
- System Integrator’s Guide
- Issues

Background

- Briefed NTAG on COE and Windows 2000 at November 2000 meeting
- Submitted updated I&RTS Chapter 7 and Appendix B to DISA in December 2000
- NTAG, DII COE Chief Engineer and staff reviewed the new material on 28 Feb 2001
- Directed to split out Windows 2000 related guidance:
  - Chapter 7: Windows segmentation guidance
  - Chapter 9: Windows developer guidance
  - Chapter 6: Common guidance
  - Directory Services Chapter section: Active Directory guidance
  - Appendix B: Compliance check items
  - System Integrator's Guide section

Background (con't)

- Draft materials sent out for review are content complete but require a lot of format and reference clean up before release
- Goal is to collect NTAG member comments today on the content then finalize I&RTS 4.2 and deliver to Dr. Lawrence by 25 May

Chapter 7

- Adoption of Logo Specifications
  - Desktop - Application Specification for Microsoft Windows 2000 for desktop applications.
  - Server – Application Specification for Microsoft Windows 2000, Server, Advanced Server, and DataCenter Server.
- COE will support
  - Windows 2000 Professional (Workstation);
  - Windows 2000 Server; and
  - Windows 2000 Advanced Server
- COE will not support
  - Datacenter Server
  - Appliance Kit

Chapter 7 (con’t)

- Segments that contain hardware device drivers shall at a minimum support Windows 2000; device drivers for Windows NT/95/98 are optional.
- Windows Installer
  - MSI installation packaging required by Logo
  - Abbreviated segments only
  - The included Setup.exe file shall check to see if the operating system is Windows NT and if it is and the Windows Installer service is not installed, then installs the Windows Installer service.

Chapter 7 (con't)

- Windows Installer (con't)
  - Ability to display the segments `ReleaseNotes`
  - Ability to display the segments software and/or hardware conflicts
  - Ability to display the segments software and/or hardware dependencies
  - Ability to display a Help screen, which details the installation procedures.
  - A `Next` button event sequence that validates any dependency and/or conflict before displaying the next screen.

Chapter 7 (con’t)

- Windows Installer (con’t)
  - Display the segments name, prefix, and version number
  - Provide batch file that can be used to initiate a silent/unattended installation of the segment.
- Being a Windows operating system core component does not mean the DII COE endorses their use.

Chapter 9

- New section; *9.6 Windows-unique Considerations*
- Hardware Device Drivers
  - device drivers should have a digital signature from the Windows Hardware Quality Labs
  - Developers and programs should submit the Windows 2000 driver for distribution on the Microsoft Windows Driver Library (WDL).
- New GUI guidelines:
  - *Windows User Experience, Official Guidelines for User Interface Developers and Designers*

Chapter 9 (con't)

- Two exceptions to Logo Specifications
  - Support for Autoplay: segments are not required to obtain a waiver to not support the CD-ROM Autoplay requirement.
  - Option to implement Active Directory schema changes: The Logo Server Specification allows creation of new objects and attributes from within the segment or as a separate installation package. All COE schema changes shall be implemented using a separate server installation package.

Chapter 9 (con't)

- Windows Management Instrumentation (WMI)
  - Client WMI Requirement

    Client management applications should use the Component Object Model (COM) to interface with WMI.
  - WMI Provider Requirements
    - Device drivers shall ensure the device's resource objects are exposed to the WMI infrastructure.
    - Segments with WMI providers shall use the existing CIM (with WMI subclasses) management objects, however they may create additional subclasses if required.

Chapter 6

- Segment Suite's
  - Member segments
  - Sub-components
    - Required or
    - Optional
  - Each member segment in a segment Suite is capable of operating independently of the other member segments

Chapter 6 (con't)

- Directory structure
  - Suites home directory

    ```
    Segment drive:\Program Files\SegDir
    ```

  - Child segments are under ..\SegDir
  - Shard files

    ```
    Segment drive:\Program Files\Common Files\
      SegDir
    ```

  - SegDir is the DISA assigned suite directory's name

Chapter 6 (con’t)

- Each segment’s matching segment descriptor files shall be packaged based on the member segment's type
- Each member segment shall specify a dependency on the Suite segment.

Directory Services Chapter

- Active Directory schema contains two primary items:
  - object class
  - attribute
- Object class represents a category of objects that share a set of common characteristics
- Attributes used to describe instances of the class
- Directory schema is self describing
  - Classes are described in the classSchema class
  - Attributes are described in the attributeSchema class
- Attributes are classified as mandatory and optional
- Linked Attributes - can link a new attribute to an existing attribute, e.g., User Manager => User Reports. Links must have a unique link identifier.

Directory Services Chapter (con't)

- Object Classes and Attributes have common characteristics
  - Object Identifier (OID), used intra directory
  - Class-Name (cn)
  - LDAP-Display-Name
  - Global Unique Identifier (GUID), 128 bit number used inside Active Directory

Directory Services Chapter (con't)

- Object Identifier
  - Must be unique
  - Issued by ISO who owns the international LDAP root OID
  - ANSI issues OIDs in North America for ISO
    - **1.2.840**
  - Microsoft has root OID from ANSI
    - **1.2.840.113556**
  - Microsoft does issue OID roots to companies that are derived from their root
  - Number of root OIDs is a performance issue. Goal should be to minimize the number of root OIDs.

Directory Services Chapter (con't)

- Each Service, CINC, or agency should determine their own Active Directory topology.
- All CINCs, Services and agency's Active Directory implementations shall share a common Active Directory global catalog schema.
- CINCs, Services and agencies determine Universal group naming conventions.
- CINCs, Services and agencies determine distribution group naming conventions.

Directory Services Chapter (con't)

- Common-Name (cn)

  Format: [prefix]-[Application or System name]-[Description]

- LDAP-Display-Name (lDAPDisplayName)

  Format: [prefix]-[Application or System name Description]

Common-Name	LDAP-Display-Name
af-mil-AIMNT-Connection-Point	afmil-AIMNTConnectionPoint
usmc-mil-C2PC-Gateway-Servers	usmcmil-C2PCGatewayServers
army-mil-ABCS-COP-Dist-Points	armymil-ABCSCOPDistributionPoints
mil-GBS-Transmission-Servers	mil-GBSTransmissionServers

Directory Services Chapter (con't)

- Globally Unique Identifier (GUID)

  Globally Unique Identifiers for new objects and attributes should be created and assigned by the developing organization.

- With one exception the cognizant Chief Engineer shall approve all schema changes.
- Active Directory schema changes shall be coordinated with the DISA Chief Engineer for Directory Services prior to implementation.

Directory Services Chapter (con't)

- Deriving a new subclass from an existing class does not require Chief Engineer approval, i.e.,
  - Connection Point,
  - Service Connection Point,
  - Service Administration Point and
  - Service Instance.
- If the new class adds new attributes to the schema then Chief Engineer approval is required.

Directory Services Chapter (con't)

- Creation of the new objects and attributes or the creation of another instance of an existing object shall be done from within a separate server installation package in accordance with the Logo Server Specification.
- Developers may obtain link-Id's from the DISA Engineering Office.

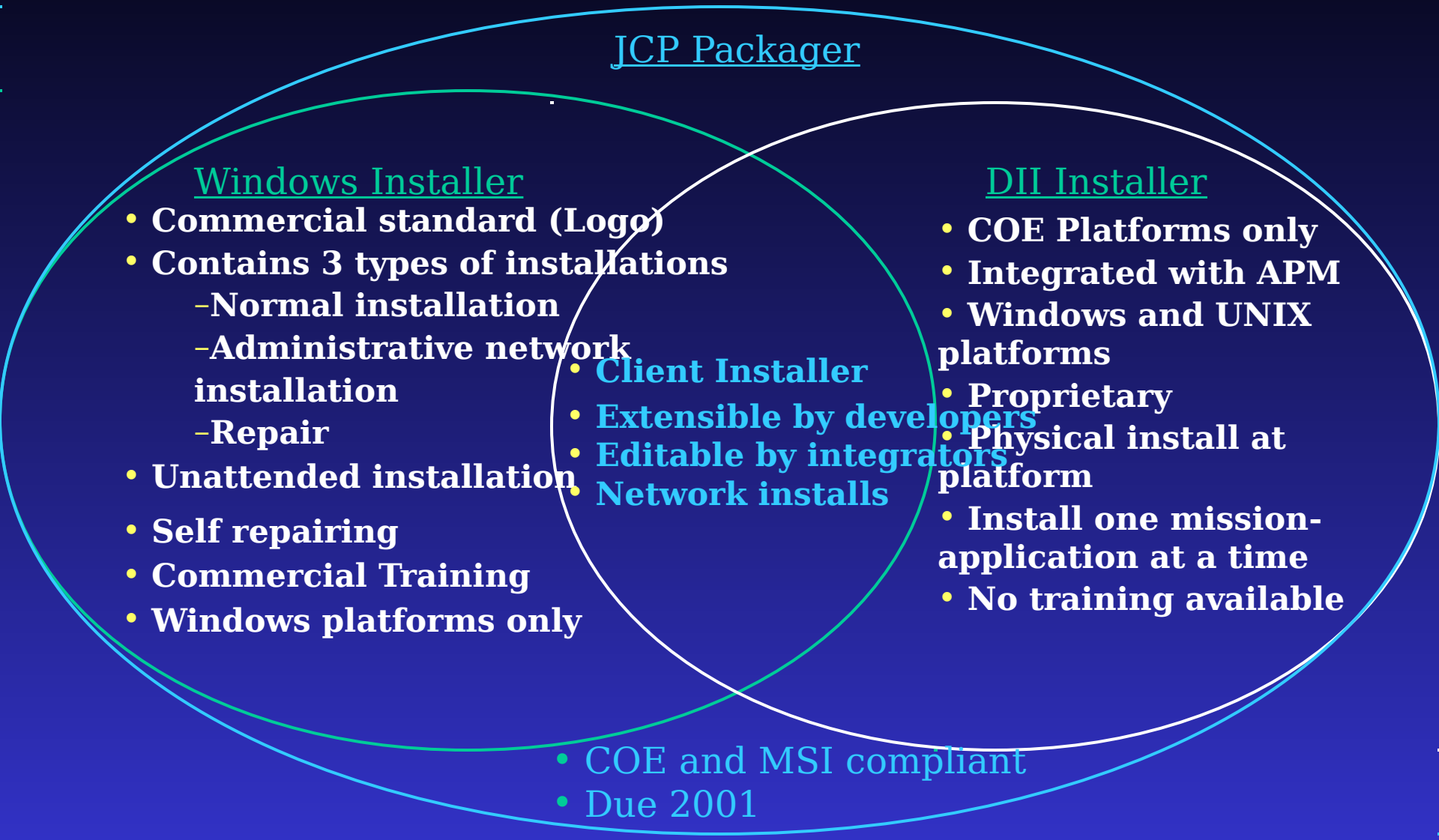
System Integrator’s Guide

- Moved from Chapter 7
  - DHCP
  - Partition structure for Workstation and Server
  - User directory Structure
  - Domains NT & Win2k
  - Win2k
    - Tree
    - Forest
  - Groups
  - Network based client devices

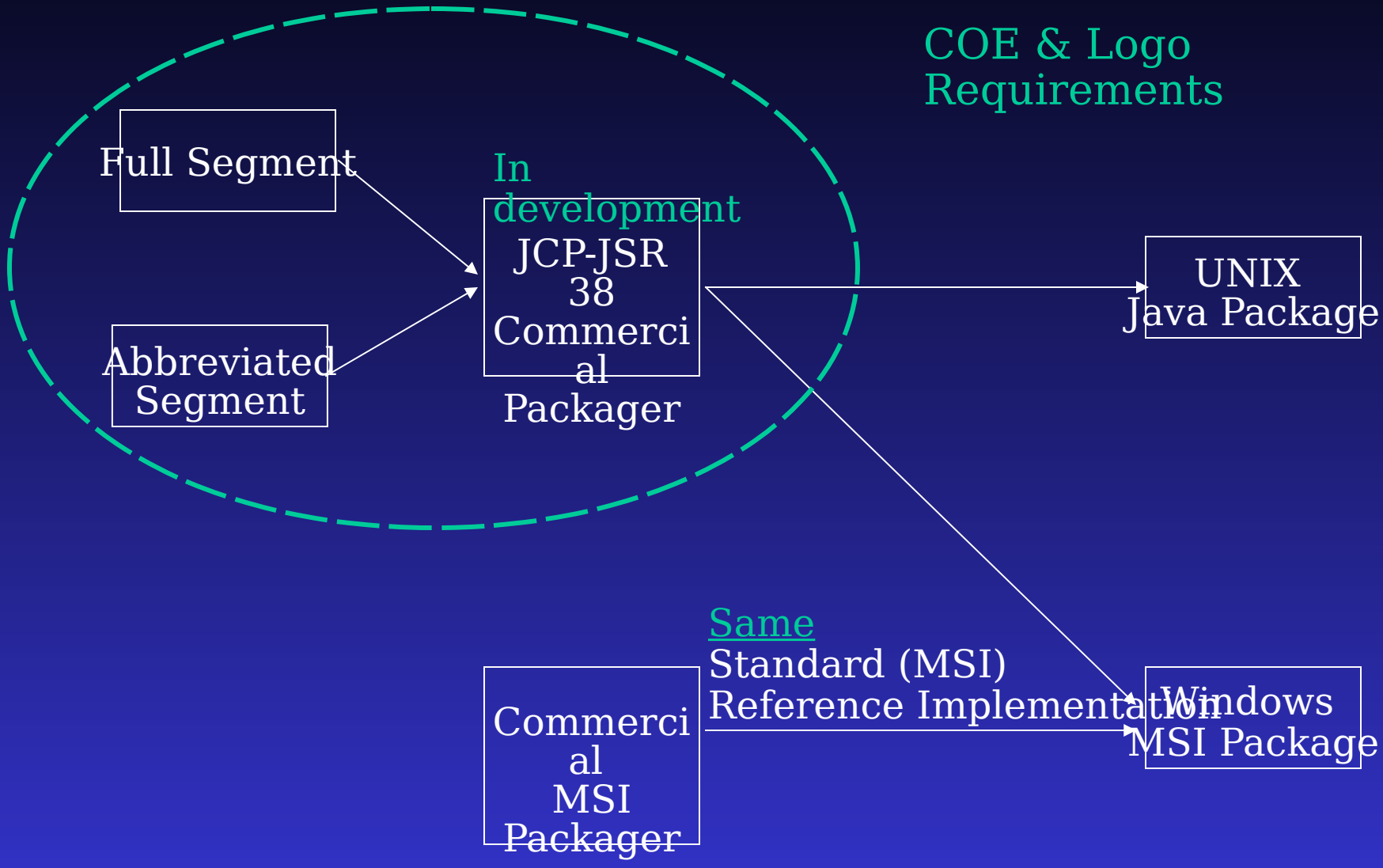
Issues

- Installation Technologies: COE on the Windows platform will adopt the Windows Installer IAW Windows Logo Program
  - A complex issue that has many implementation details that still need to be addressed
  - Draft I&RTS still says full segmentation required
- Dividing current kernel into:
  - Baseline and
  - Tier 1
- Terminal server

Installation Technologies



COE Full Segment Migration Process



Why a Baseline

- The need for a standard configuration:
  - Security
  - Administration
  - Backup
- OASD tasked DISA to build and deploy a Windows Baseline
- COE version 5 scheduled to split kernel into Baseline and Tier 1 segments

What the Baseline does

- Operational configuration for Windows NT and Windows 2000
  - New systems
  - Existing systems
- Security configuration for Windows NT and Windows 2000
  - Baseline - for all Windows platforms in DoD
  - Secure - current COE C2 level configuration
  - High Secure - set by Program, CINC, Service or Agency

Proposed COE 4.6 Architecture

Tier 1

- COE Kernel Utilities
- Permission Display Engine
- COE Java Runtime
- Icon Display Tool
- Directory Access
- Common Data Store
- Account and Profile Manager
- COEInstaller

Baseline

- Operational Configuration
- Security Configuration

Delta Between Baseline and Kernel

	Baseline	Kernel	
• COE Kernel Utilities		X	
• Permission Display Engine		X	
• COE Java Runtime		X	
• Icon Display Tool		X	
• Directory Access		X	
• Common Data Store		X	
• Account and Profile Manager			X
• COEInstaller			X
• I&RTS Partition Requirement		X	
• Military Time		X	
• DISA Splash screen	X	X	
• DoD Legal screen	X	X	
• Baseline Security configuration		X	
• C2 (-) Security configuration		X	X
• Security Administration		X	
• Low Light display schemas			
• Security level registry entry	X		
• Install Security Editor (NT only)		X	

Terminal Server

- Issue: COE does not support terminal server
- Separate product in NT
- Integrated into Windows 2000 server family
- Integrated into Windows XP Professional